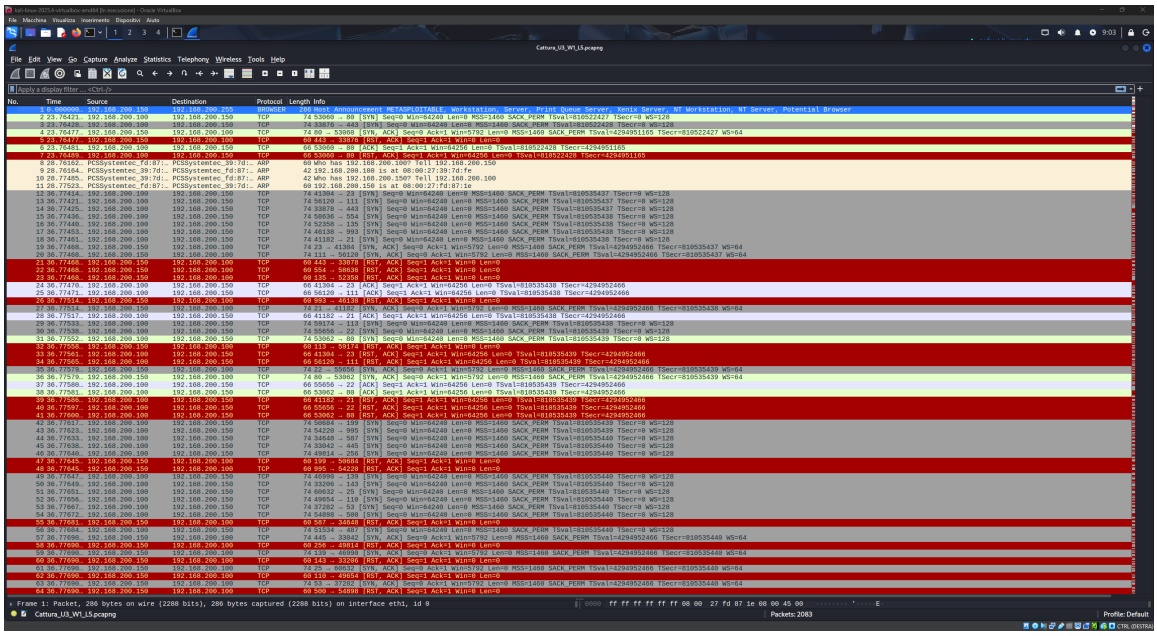
Report Tecnico:
Network Traffic Analysis

Forensic Analysis of TCP Port Scanning Activity

Studente: Josh Van Edward D Abanico
Data: 6 febbraio 2026



Oggetto: Analisi Forense - Port Scanning Detection
Tool Utilizzato: Wireshark

Indice

1 Introduzione e Scenario Operativo

1.1 Obiettivi dell'Analisi

Il presente documento riporta l'analisi tecnica di una cattura di traffico di rete (PCAP). L'obiettivo primario è caratterizzare la tipologia di traffico anomalo rilevato tra due host della rete locale, identificare le tecniche di ricognizione utilizzate dall'attaccante e mappare la superficie di attacco esposta dalla vittima.

1.2 Topologia della Rete Ricostruita

Dall'analisi dei pacchetti ARP (Address Resolution Protocol) e del traffico TCP, è stata definita la seguente topologia:

- **Attaccante (Scanner):** `192.168.200.100`
- **Vittima (Target):** `192.168.200.150`
- **Asset Inventory:** Il target è identificato come una macchina virtuale "Metasploitable 2", progettata intenzionalmente con vulnerabilità per scopi di testing (banner rilevato nel pacchetto n. 1).

2 Fase 1: Analisi Cronologica dell'Attacco

2.1 Annuncio Spontaneo della Vittima

Al pacchetto n. 1 (Time 0.000), la macchina vittima invia un messaggio broadcast **NetBIOS Host Announcement**, rivelando spontaneamente la propria presenza e il proprio nome host ("METASPLOITABLE") all'intera rete, senza alcuna sollecitazione esterna.

2.2 Verifica Attività (TCP Ping)

Circa 5 secondi prima della scansione principale (pacchetti 2-7), l'attaccante esegue un controllo di disponibilità ("Host Discovery") per verificare se il target è attivo. Vengono inviati pacchetti **SYN** mirati verso le porte standard **80 (HTTP)** e **443 (HTTPS)**.

- La ricezione di un `[SYN, ACK]` dalla porta 80 (pacchetto 4) conferma all'attaccante che l'host è acceso e raggiungibile.
- L'attaccante chiude immediatamente la connessione preliminare con un `RST` (pacchetto 7), avendo ottenuto la conferma necessaria per procedere con l'attacco massivo.

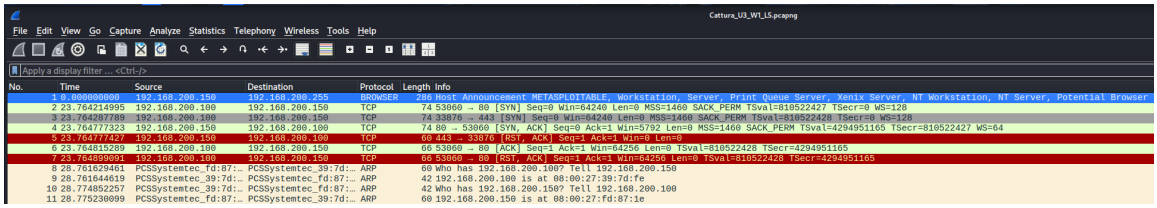


Figura 1: Pre-Attacco: Host Announcement spontaneo e TCP Ping di verifica (Porte 80/443).

2.3 Network Discovery (ARP)

L'attività ostile inizia con una fase di discovery locale. L'host attaccante esegue richieste ARP broadcast ("Who has 192.168.200.150?") per risolvere l'indirizzo fisico (MAC Address) della vittima, preludio necessario a qualsiasi comunicazione IP diretta.

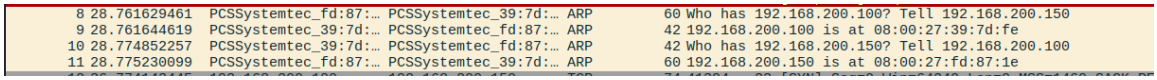


Figura 2: Richieste ARP broadcast.

2.4 Attacco alle "Top Ports" (Initial Burst)

Immediatamente dopo aver ottenuto il MAC Address della vittima (pacchetto 11), l'attaccante lancia una raffica simultanea di richieste `[SYN]` verso le porte TCP più comuni ("Top Ports"), visibile dal pacchetto 12 al 18. Questa fase è mirata a identificare rapidamente i servizi standard prima di procedere con una scansione completa.

L'analisi dei pacchetti di risposta (dal 19 al 41) permette di delineare immediatamente il profilo di sicurezza della vittima:

- **Servizi Aperti (Open):** La vittima risponde `[SYN, ACK]` sulle porte **21 (FTP)**, **23 (Telnet)**, **80 (HTTP)**, **111 (RPC)** e **22 (SSH)**.
- **Servizi Chiusi (Closed):** La vittima invia un `[RST, ACK]` per le porte cifrate o più moderne come **443 (HTTPS)** e **993 (IMAPS)**.

1. **Riga 12:** Attaccante invia SYN.
2. **Riga 19:** Vittima risponde SYN, ACK.
3. **Riga 24:** Attaccante invia **ACK** (Connessione stabilita).
4. **Riga 33:** Attaccante chiude con RST, ACK.

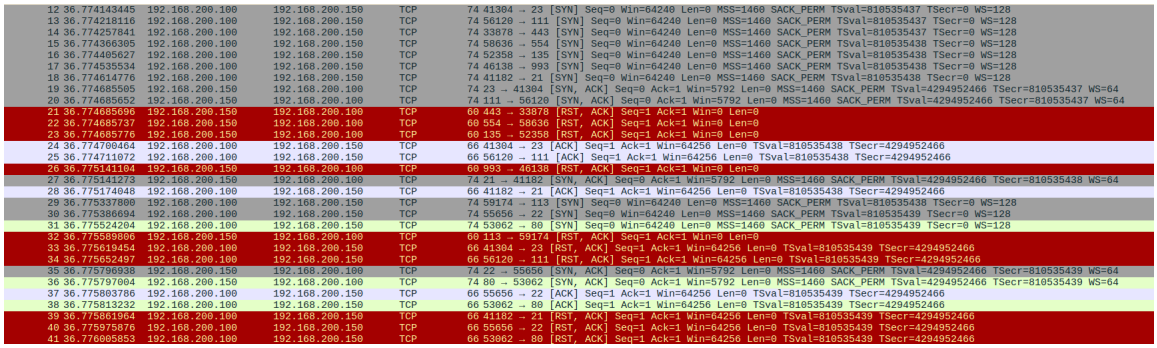


Figura 3: Raffica iniziale sulle porte principali: evidenza delle porte aperte (Telnet, FTP, HTTP) e chiuse (HTTPS).

2.5 Enumerazione Infrastruttura e Mail (Second Wave)

Proseguendo la scansione (dal pacchetto 42 in poi), l'attaccante sposta il focus dai servizi di accesso remoto ai servizi di infrastruttura e condivisione file. Questa fase evidenzia una chiara distinzione tra i protocolli supportati dalla macchina vittima.

L'analisi del traffico mostra:

- **File Sharing (Critico):** Vengono rilevate aperte le porte **139 (NetBIOS-SSN)** e **445 (Microsoft-DS)**. La presenza della porta 445 aperta su un sistema Linux/Unix (come indicato dal banner iniziale) suggerisce la presenza del servizio **Samba**, un vettore di attacco frequente per vulnerabilità di tipo RCE (es. SambaCry).
- **Servizi Mail:** È presente una configurazione parziale. La porta **25 (SMTP)** risulta aperta (pacchetto 62), mentre i protocolli di ricezione posta (**POP3 porta 110**, **IMAP porta 143**) e le varianti sicure (**995, 587**) vengono rifiutati con un RST dalla vittima.
- **DNS:** Viene rilevata aperta anche la porta **53 (Domain Name System)**.

Evidenza Tecnica: Le righe 66-68 dello screenshot mostrano nuovamente l'invio dei pacchetti **ACK** da parte dell'attaccante verso le porte 445, 139, 25 e 53. Questo conferma che anche per i servizi infrastrutturali è stata utilizzata una connessione TCP completa, lasciando tracce evidenti nei log del servizio Samba e del Mail Transfer Agent.

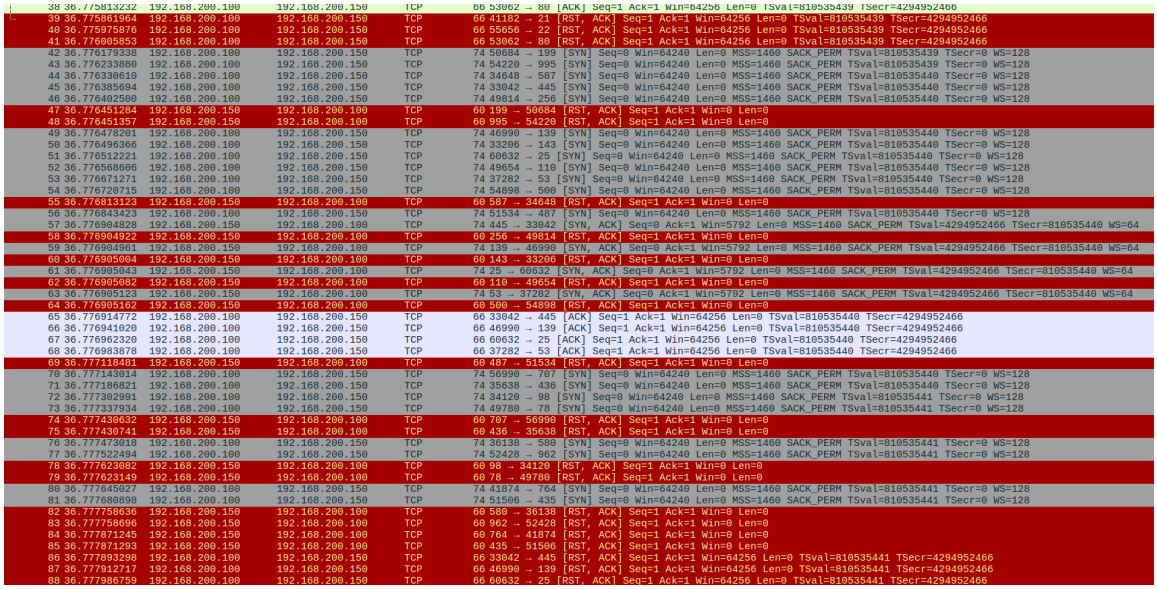


Figura 4: Seconda ondata: Rilevamento di Samba (445), NetBIOS (139) e SMTP (25).

2.6 Chiusura Sessioni e Noise Scanning

Immediatamente dopo aver completato l'handshake TCP sulle porte target (fase precedente), l'analisi del traffico evidenzia la fase di "Teardown" (smantellamento) delle connessioni. Nello screenshot , alle righe **86-89**, l'attaccante invia pacchetti **RST, ACK** verso le porte precedentemente confermate aperte:

- **Porta 445 (SMB)**
- **Porta 139 (NetBIOS)**
- **Porta 25 (SMTP)**
- **Porta 53 (DNS)**

Questa azione conferma la natura automatizzata dell'attacco: il tool apre la connessione solo per verificarne l'esistenza e la chiude immediatamente (circa 10ms dopo l'apertura) per minimizzare l'impiego di risorse, pur lasciando traccia nei log.

2.7 Rilevamento Servizi Legacy Critici (Porta 512)

L'analisi approfondita del traffico ha permesso di isolare un evento di sicurezza ad alta criticità che era passato in secondo piano durante la scansione massiva.

Alle righe **164-166**, si osserva il rilevamento della porta TCP **512**.

- **Contesto:** La porta 512 (tcp/exec) fa parte della suite di comandi "R" (r-commands) di Unix/Linux. È un servizio di esecuzione remota noto per la sua debolezza intrinseca (spesso basata solo sull'autenticazione dell'indirizzo IP tramite file `.rhosts`, senza richiesta di password).

Dinamica dell'Handshake (Evidence): Anche in questo caso, la sequenza dei pacchetti conferma la tecnica *Connect Scan* e l'avvenuto contatto con il servizio:

1. **Packet 164:** La vittima risponde `[SYN, ACK]` dalla porta 512. Il servizio è attivo e in ascolto.
2. **Packet 165:** L'attaccante invia un `[ACK]` (evidenziato in bianco/blu nello screen). Questo completa la connessione TCP.
3. **Packet 170:** L'attaccante invia `[RST, ACK]` per chiudere la connessione.

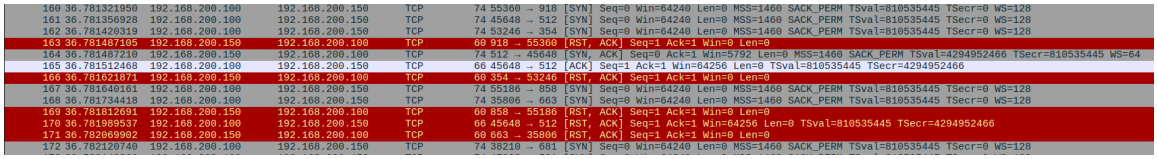


Figura 5: Discovery della porta critica 512 (exec). Il pacchetto 165 (ACK) conferma l'avvenuta connessione.

2.8 Conferma Vulnerabilità R-Services (Porta 514)

Pochi millisecondi dopo la scoperta della porta 512, l'analisi del traffico evidenzia l'apertura di un ulteriore servizio critico correlato.

Alla riga **267**, la vittima risponde positivamente a una richiesta di connessione sulla porta TCP **514**.

- **Identificazione Servizio:** La porta 514 TCP è standard per il servizio **shell** (cmd). Insieme alla porta 512 (exec) identificata in precedenza, conferma la presenza attiva della suite "R-Services" (rsh, rlogin, rcp).

Anche in questo frangente, il pacchetto n. 268 (**ACK**) certifica che la connessione è stata pienamente stabilita prima di essere resettata (pacchetto 273), lasciando traccia dell'intrusione nei log del demone inetd/xinetd.

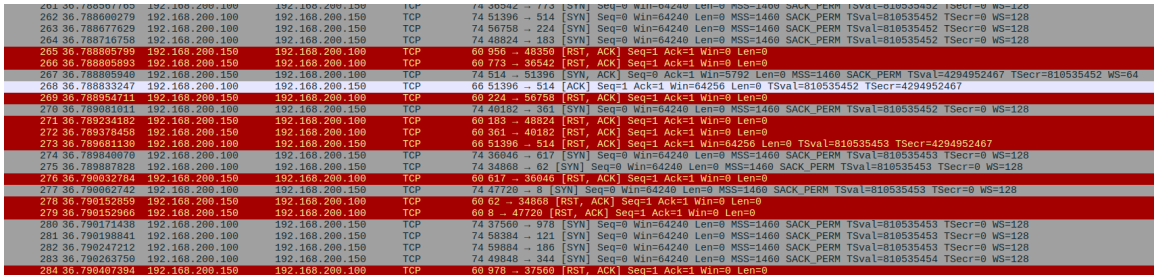


Figura 6: Rilevamento della porta 514 (shell), confermando l'esposizione della suite R-Services.

2.9 Identificazione R-Login (Porta 513)

L'analisi del traffico prosegue rivelando l'ultimo componente della suite di servizi di amministrazione legacy. Si osserva l'handshake completo sulla porta TCP **513**.

- **Packet 988:** L'attaccante invia la richiesta `[SYN]` verso la porta 513.
- **Packet 994:** La vittima accetta la connessione inviando `[SYN, ACK]`.

- **Packet 997:** L'attaccante finalizza la connessione con `[ACK]`.

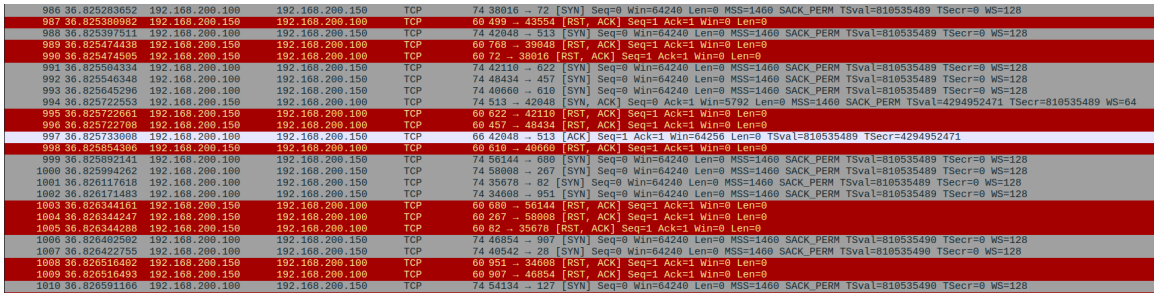


Figura 7: Rilevamento del servizio rlogin (Porta 513), che completa la triade dei servizi R vulnerabili.

Successivamente, il traffico è caratterizzato da quello che in gergo forense viene definito "Scanning Noise": una serie di tentativi verso porte non standard o casuali (es. 148, 806, 221, 206) che rispondono invariabilmente con **RST, ACK** (rifiuto), indicando che nessun servizio è in ascolto su di esse.

Estensione dell'Attacco: È fondamentale notare che questo comportamento persiste per tutta la durata residua del file di cattura. L'attaccante ha continuato sistematicamente a scansionare l'intero range di porte (o un sottoinsieme molto vasto), generando un flusso continuo di risposte `[RST, ACK]` (visibili come un "muro rosso" in Wireshark) per tutte le restanti porte non attive.

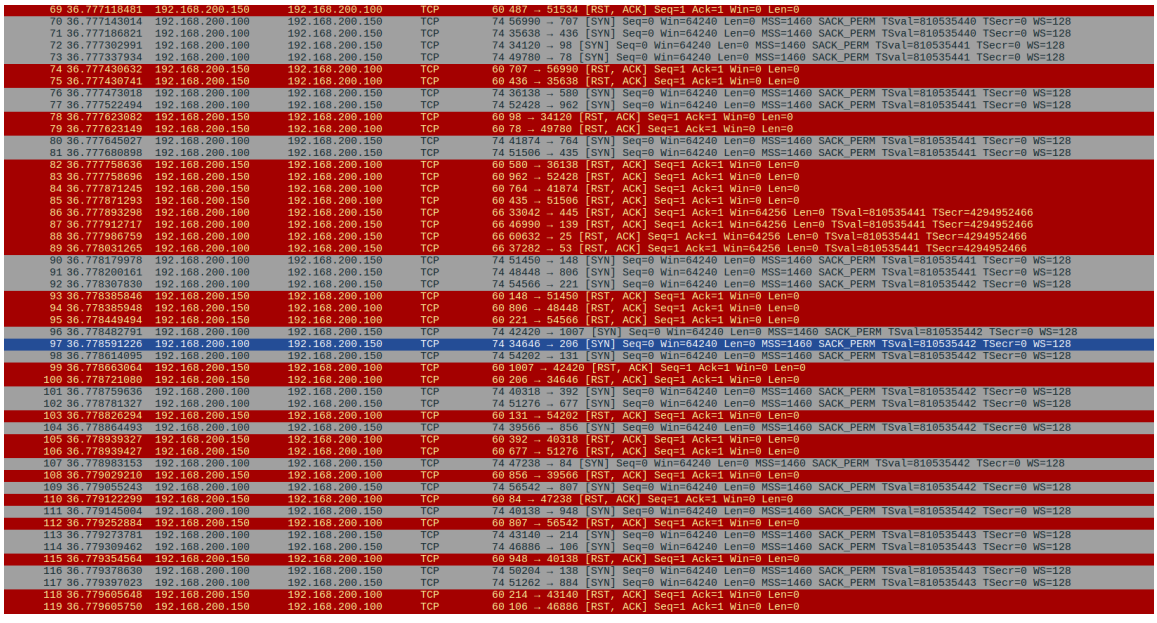


Figura 8: Teardown delle connessioni (RST su porte aperte) e prosecuzione su porte chiuse (Noise).

3 Fase 2: Approfondimento Tecnico (Stealth vs Connect)

Questa sezione dettaglia l'analisi forense che ha permesso di determinare l'esatta tipologia di scansione utilizzata.

3.1 Differenze Teoriche: TCP Connect vs SYN Stealth

Per comprendere l'analisi, è fondamentale distinguere le due modalità principali di scansione TCP:

TCP Connect Scan (-sT)	**SYN "Stealth" Scan (-sS)**
Esegue il *Three-Way Handshake* completo.	Esegue un handshake parziale (Half-open).
Flow: SYN → SYN/ACK → **ACK** → RST	**Flow:** SYN → SYN/ACK → **RST**
La connessione viene stabilita a livello Applicativo.	La connessione viene interrotta prima di essere stabilita.
Rilevabilità: Alta. Viene registrata nei log di sistema della vittima.	**Rilevabilità:** Bassa. Spesso invisibile ai log applicativi standard.

Tabella 1: Confronto tecnico tra le tipologie di scansione.

3.2 Analisi Forense

Analizzando la cattura Wireshark, abbiamo isolato la sequenza di pacchetti relativa alla porta **445 (SMB)**, visibile nello screenshot di prima.

La sequenza osservata è la seguente:

1. **SYN (Attaccante → Vittima):** Richiesta di connessione.
2. **SYN, ACK (Vittima → Attaccante):** Conferma disponibilità della porta.
3. **ACK (Attaccante → Vittima):** *Il punto decisivo.* L'attaccante invia il pacchetto ACK (pacc. n. 66), completando la connessione.
4. **RST, ACK (Attaccante → Vittima):** Solo successivamente (pacc. n. 86) la connessione viene abbattuta.

3.3 Deduzione Investigativa

La presenza del pacchetto **ACK** (terzo step dell'handshake) conferma in modo incontrovertibile che si tratta di una **TCP Connect Scan**. Se fosse stata una scansione Stealth, l'attaccante avrebbe inviato un RST immediatamente dopo aver ricevuto il SYN, ACK, senza mai inviare l'ACK finale.
L'analisi dei pacchetti permette di ricostruire con elevata probabilità le opzioni utilizzate nel tool di scansione (Nmap).

1. **Tecnica (-sT):** La presenza del pacchetto **ACK** inviato dall'attaccante (terzo step dell'handshake) prima del RST conferma l'uso della **TCP Connect Scan**. Se fosse

stata una scansione "Stealth" (SYN Scan, default per root), avremmo visto un RST subito dopo il SYN-ACK della vittima.

2. **Estensione (-p-):** L'elevato volume di traffico registrato verso porte non standard e tipicamente chiuse (es. tentativi TCP sulla porta 138, solitamente UDP, o porte randomiche come 118 e 806) indica che l'attaccante non si è limitato alle "Top 1000" porte, ma ha verosimilmente lanciato una scansione sull'intero range di porte (1-65535).
3. **Timing:** La densità temporale dei pacchetti (inviati a intervalli di microsecondi) suggerisce l'uso di un template di timing aggressivo (es. -T4).

Comando Ipotizzato: Sulla base delle evidenze, il comando eseguito dall'attaccante è riconducibile alla seguente sintassi:

```
nmap -sT -p- 192.168.200.150
```

Implicazioni di Sicurezza: L'utilizzo della flag `-sT` rende l'attacco estremamente "rumoroso". Poiché ogni connessione verso le porte aperte è stata completata a livello di socket, è altamente probabile che i demoni dei servizi (FTP, SSH, Samba) abbiano registrato l'IP dell'attaccante nei log di sistema della vittima (`/var/log/auth.log`, `/var/log/samba/`, ecc.), permettendo una facile attribuzione dell'attacco.

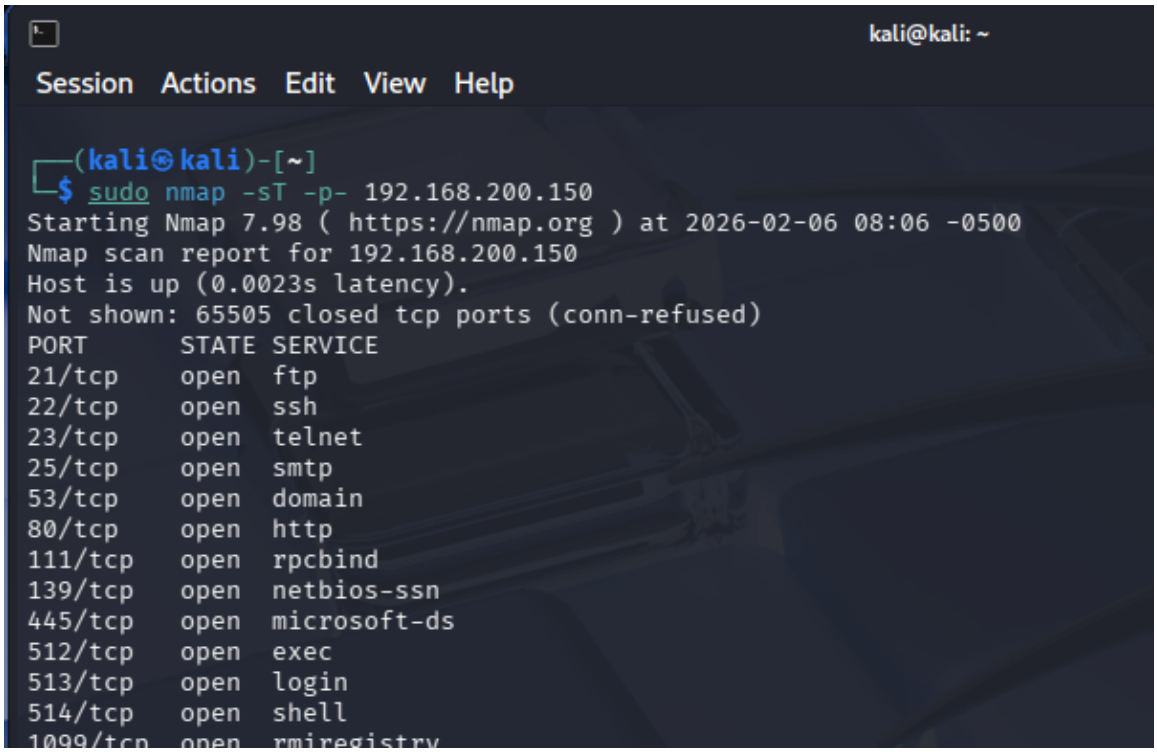


Figura 9: Comando probabilmente usato dalla Kali vero la Metasploitable.

4 Fase 3: Risultati dell'Enumerazione

L'attività di scansione ha avuto pieno successo, permettendo all'attaccante di mappare l'intera superficie di attacco. Di seguito sono elencati i servizi confermati come **OPEN**, suddivisi per tipologia e livello di rischio.

4.1 Criticità Massima: Suite "R-Services" (Legacy)

L'analisi ha rilevato l'esposizione della suite completa dei comandi Unix legacy "Berkeley r-commands". Questi servizi sono considerati ad altissimo rischio poiché spesso basano l'autenticazione solo sull'indirizzo IP di provenienza (trust relationship), permettendo accessi root senza password.

- **Porta 512 (TCP exec):** [Rilevata nel pacchetto 165]. Permette l'esecuzione remota di comandi. È il vettore principale per attacchi RCE immediati.
- **Porta 513 (TCP login):** [Rilevata nel pacchetto 994]. Servizio *rlogin*, equivalente non cifrato di Telnet/SSH, ma con meccanismi di trust deboli.
- **Porta 514 (TCP shell):** [Rilevata nel pacchetto 267]. Servizio *rsh* (remote shell). La presenza contemporanea di exec, login e shell conferma che il sistema è obsoleto e non sicuro.

4.2 File Sharing e Infrastruttura

Sono stati identificati servizi che espongono il file system o gestiscono risorse di rete, vettori ideali per l'esfiltrazione di dati o attacchi laterali.

- **Porta 445 (SMB) e 139 (NetBIOS):** Servizi per la condivisione file Windows/-Samba. Su sistemi Linux datati, la porta 445 è spesso vulnerabile a exploit critici (es. SambaCry o translatable SID).
- **Porta 21 (FTP):** File Transfer Protocol. Servizio in chiaro, vulnerabile a sniffing delle credenziali e, in alcune versioni (es. vsftpd 2.3.4), contenente backdoor.
- **Porta 111 (RPCbind):** Mappa i servizi RPC su porte di rete. Utile all'attaccante per enumerare ulteriori servizi (come NFS).
- **Porta 25 (SMTP):** Mail Server. Configurato per l'invio, ma con le porte di ricezione (POP3/IMAP) chiuse.
- **Porta 53 (DNS):** Servizio di risoluzione nomi.

4.3 Accesso Remoto e Web

- **Porta 23 (Telnet):** Accesso amministrativo remoto obsoleto. Tutto il traffico, incluse user e password, viaggia in chiaro.
- **Porta 80 (HTTP):** Web Server. Potenziale superficie per attacchi web-based (SQL Injection, XSS, CGI vulnerabilities).
- **Porta 22 (SSH):** L'unico servizio di amministrazione cifrato rilevato, sebbene possa essere soggetto ad attacchi Brute Force.

5 Conclusioni

L'analisi forense ha confermato che l'host `192.168.200.150` è stato oggetto di una **TCP Connect Scan** massiva proveniente dall'IP `192.168.200.100`. Poiché l'attaccante ha completato le connessioni TCP (Three-way handshake), l'attività è stata tracciata nei log di sistema della vittima, rendendo l'attacco facilmente attribuibile.

Valutazione del Rischio: CRITICA La scansione ha rivelato una compromissione totale della sicurezza perimetrale. I vettori di attacco più gravi identificati sono:

- **Suite R-Services (Porte 512, 513, 514):** Presenza di servizi legacy che permettono l'accesso *root* senza password.
- **File Sharing (Porta 445):** Rischio elevato di esecuzione codice remoto (es. SambaCry).
- **Protocolli in Chiaro (21, 23):** Credenziali esposte a sniffing.

Azioni Richieste: Isolare immediatamente l'host, analizzare i file di log (es. `/var/log/auth.log`) per confermare eventuali accessi abusivi successivi alla scansione e chiudere le porte non essenziali.